



## Visa U.S.A. Inc. Data Security Alert

June 27, 2006

To support compliance with the Visa U.S.A. Cardholder Information Security Program, Visa is committed to helping all payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security alerts when vulnerabilities are detected in the marketplace.

Members may share this alert with their merchants, agents, and other parties as a confidential communication to help ensure they are aware of emerging vulnerabilities and take appropriate steps to mitigate risk.

### Security Vulnerability

#### ***Improperly Installed Point of Sale (“POS”) Systems***

It has come to the attention of Visa that small to mid-sized restaurants and other merchants may be exposed to compromise attacks due to vulnerabilities caused by mis-configured POS systems.

POS systems that are not properly installed or adequately maintained can contribute to the compromise of cardholder account information and other sensitive data.

Often, merchants use third-party firms known as “integrators” or “resellers” to configure or install POS systems. Because third-party firms may vary in their ability to properly install and configure common security controls, POS systems may be vulnerable to compromise upon installation. Merchants are urged to begin a dialogue with their vendors to ensure their POS systems are adequately safeguarded from internal and external intrusions.

### ***Recommended Mitigation Strategy***

To safeguard their POS systems, merchants should ask their POS vendors (i.e. resellers / integrators) the following questions.

1. Does my POS software store magnetic stripe data (e.g., track data) or PIN blocks? If so, this is prohibited and must be immediately corrected.
2. Does my network have a properly-configured firewall installed to protect my POS system from unauthorized access?
3. Are complex and unique passwords required to access my system? Can the POS vendor confirm they don't use a common or default password across other merchant systems they support?
4. Does my POS system enable the POS vendor to have remote access for support or maintenance? If so, merchants must ensure appropriate controls are implemented to prevent unauthorized access.
5. Is the POS system configured so that access to critical functions may be restricted?
6. Is the POS system used for payment card processing used for other functions? If so, the POS system must be segregated from other functions. (i.e. Web browsing / e-mailing)
7. Is the operating system hosting the POS software patched with the applicable security updates in a timely manner?
8. Has my POS software version been validated as compliant against the Visa Payment Application Best Practices (“PABP”) ? A list of PABP compliant applications is available on <http://www.visa.com/cisp>.

**For more information on Visa's Cardholder Information Security Program, please visit <http://www.visa.com/cisp>. Questions about this alert may be directed to [CISP@Visa.com](mailto:CISP@Visa.com)**

Alert 062706